

generating rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.

- 5     29.            (Twice Amended) A method of generating a security policy for a network, said network including a plurality of hosts, said method comprising the steps of:
- receiving a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of said network, such that said hosts inherit said definitions associated with an assigned role;
- 10                   receiving an assignment of said roles to said hosts in said network; and
- generating said security policy from said received definitions and assignments.
35.                (Twice Amended) A compiler for generating a configuration file for a firewall in a network, said network including a plurality of hosts, comprising:
- 15                   a memory for storing computer-readable code; and
- a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:
- receive a definition for a plurality of roles that specify the ability of a host to send and receive packets, wherein each of said roles may be assigned to said hosts independently of a topology of
- 20     said network, such that said hosts inherit said definitions associated with an assigned role;
- receive an assignment of said roles to said hosts in said network; and
- generate rules for said hosts based on said assigned roles, said rules determining whether a packet is passed to a destination host.
- 25     38.            (Twice Amended) A system for generating a security policy for a network, said network including a plurality of hosts, said system comprising:
- a memory for storing computer-readable code; and
- a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to: